

A Blockchain-Based Model for Secure Academic Transcript Transfer

Author

Daisy Jeruto Limo ⁽¹⁾; Nelson Masese ⁽²⁾; Alex Kibet ⁽³⁾

Main author's email: daisyjeruu@gmail.com

(1,2) Kabarak University, Kenya; (3) Laikipia University, Kenya.

Cite this article in APA

Limo, D. J., Masese, N., & Kibet, A. (2026). A blockchain-based model for secure academic transcript transfer. *Journal of computer science and technology*, 4(1), 86–107. <https://doi.org/10.51317/wcrxeb24>



A publication of Editon
Consortium Publishing (online)

Article history

Received: 2026-08-06

Accepted: 2026-09-11

Published: 2026-10-08

Scan this QR to read the paper online



Copyright: ©2026 by the author(s).
This article is an Open Access article
distributed under the terms and
conditions of the Creative Commons
Attribution-NonCommercial
ShareAlike 4.0 International License
(CC BY-NC-SA 4.0).



Abstract

This study aims to develop a blockchain-based system for securely exchanging student transcripts between colleges. The project aims to address problems in existing transcript transmission procedures, including unauthorised access, manipulation, fabrication, processing delays, and incompatibility with institutional systems. The study reviews technical and institutional literature to establish the requirements of the proposed model, along with other relevant literature. The model was designed according to the design-oriented approach of Design Science Research. In this study, we propose a mechanism for off-chain storage of transcripts, verification on the blockchain and maintenance of institutional records. The architecture provides secure, efficient transfer of academic transcripts through a permissioned Ethereum-compatible network, role-based access management, cryptographic hashing, smart contract technology, and standardised data interchange. The transcript content is stored off-chain, and the blockchain is used to store cryptographically secured fingerprints and transaction details for verification and integrity. This paradigm ensures data integrity, transparency, efficiency, and interoperability through institutional authentication, authorised transfer, duplicate prevention, and transaction tracking. This work is crucial for higher education institutions as it provides a systematic technique to securely and openly transfer and validate student transcripts.

Keywords: Academic transcripts, blockchain, data integrity, interoperability, verification.

1.0 INTRODUCTION

Academic mobility refers to the movement of academic records from one institution to another to enable students to continue their education, obtain recognition of academic credits, pursue professional registration, and secure employment. Historically, academic transcripts have been transferred manually through letters, courier services, email, and centralised systems. These approaches can result in delays, errors, loss, breaches, and tampering of documents, while discrepancies among institutional systems may hinder the effective interchange and interpretation of academic records (Cheung et al., 2021; Rustemi et al., 2023). Academic transcripts contain vital information, including courses undertaken, grades obtained, credit hours, and academic standing. They are therefore essential for recognising prior academic work and validating the authenticity and integrity of academic qualifications. Consequently, transcript-transfer mechanisms must be trustworthy and maintain the confidentiality and integrity of academic records while enabling institutions to exchange and verify transcripts efficiently (Al Hemaury et al., 2024; Rani et al., 2024).

Blockchain technology offers a potential solution through cryptographically linked data and a verifiable transaction history. A transcript's digital fingerprint can be established using a cryptographic hash, enabling changes to be detected by comparing the fingerprint with the original record anchored on the blockchain (Kibet & Karume, 2018). Under this approach, the transcript itself is maintained off-chain, while its cryptographic fingerprint and associated transaction metadata are anchored to the blockchain. This arrangement provides a mechanism for verifying the integrity of a transcript without exposing the complete academic record on the blockchain.

The proposed model incorporates several fundamental blockchain principles. Decentralisation enables records to be authenticated and maintained across multiple authorised institutions rather than within a single repository. Immutability ensures that a validated record entered into the blockchain cannot be altered without detection. Pseudonymity enables the use of blockchain addresses or identifiers that do not directly reveal real-world identities on the ledger. Auditability facilitates the tracking of transaction activities throughout the history of the blockchain. Smart contracts are blockchain-based programmes that can automatically enforce predefined rules governing institutional authorisation, transcript registration, verification, and the prevention of duplication. Decentralised validation further enables multiple authorised participants to validate transactions according to the rules established by the network.

Existing research has examined the application of blockchain technology to the verification of certificates, certifications, and academic credentials. Much of this research, however, focuses on credential issuance or verification rather than the complete transfer of academic transcripts across universities operating different information systems. Limited attention has been given to the integration of institutional permissions, interoperability, duplicate prevention, revocation, regulated transfer procedures, and the security of sensitive transcript data within a single framework. Consequently, a gap exists in the development of an integrated model that addresses the entire process of securely transmitting academic transcripts across institutional boundaries. The present study seeks to address this gap through the integration of institutional record management, cryptographic fingerprinting of transcripts, smart contracts, blockchain anchoring, and encrypted off-chain storage. The proposed approach provides a traceable and tamper-evident mechanism through which recognised institutions can communicate and validate academic transcripts while limiting the exposure of sensitive information on the blockchain.

The transmission of academic transcripts between higher education institutions continues to face challenges related to security, efficiency, interoperability, data integrity, and transparency. Physical, email-based, and editable electronic transfers are vulnerable to delays, forgery, and manipulation, while centralised systems may expose records to unauthorised access and alteration. Manual verification also increases administrative workload and processing time. Furthermore, differences in institutional information systems, transcript formats, grading structures, and credit rules can hinder consistent communication and interpretation of academic records. These challenges demonstrate the need for a unified framework capable of supporting the secure, efficient, and interoperable transfer and verification of academic transcripts. Therefore, this study develops a blockchain-based model that integrates institutional authorisation, cryptographic fingerprinting, blockchain verification, standardised data interchange, and secure off-chain transcript storage.

The study pursued two objectives. The first was to identify the challenges associated with academic transcript transfer between institutions, with particular focus on security risks such as unauthorised access, tampering, and forgery; efficiency-related issues, including processing delays and administrative burden; and interoperability challenges arising from differences in institutional information systems and data-exchange mechanisms. The second was to identify the design requirements and develop a blockchain-based model for the secure, transparent, and tamper-evident transfer of academic records between institutions. Correspondingly, the study addressed two research questions: What challenges are encountered in academic transcript transfer between institutions with regard to security, including unauthorised access, tampering, and forgery; efficiency, including processing delays and administrative burden; and the interoperability of institutional information systems? What design requirements are necessary for developing a blockchain-based model that supports the secure, transparent, and tamper-evident transfer of academic records between institutions?

The study makes three main contributions. First, it synthesises the challenges associated with transcript transfer into a structured problem statement organised around five key areas. Second, it derives a clear and traceable set of design criteria from these challenges, enabling each architectural decision to be linked to the vulnerability it is intended to address. Third, it presents a modular architecture that defines the smart-contract structure, the partitioning of data between on-chain and off-chain storage, the consensus configuration appropriate for a regulated institutional environment, and a functional evaluation strategy for subsequent prototype validation.

2.0 LITERATURE REVIEW

This section analyses the existing literature on the secure transfer of academic transcripts and the use of blockchain technology for academic records and credentials. The review is organised around the challenges impacting academic transcript transfer, blockchain basics, blockchain network types and consensus mechanisms, intelligent contracts and modular contract design, blockchain applications in academic credentialing, human and organisational factors, and the research gap that emerges. A review of the literature is conducted to understand how existing findings, methodologies and limitations affect the design needs of the model proposed in this work.

For this study, an academic record is defined broadly as any data an institution collects about a student's academic work and achievements. An academic transcript is the official record of academic achievement that provides precise course-level information, such as courses studied, grades or marks received, credit

hours, and academic status. Academic credentials are formal proof of educational accomplishment and include certificates and degrees. A certificate shows that you have completed or earned a specific certification. A degree is a formal academic award obtained by a college or university. Credit transfer is the recognition of academic credit obtained elsewhere by another school or program. These differences remain relevant throughout the review, as the current study focuses on the secure transfer and verification of academic transcripts, not just the granting of certificates.

Challenges in Academic Transcript Transfer

The research study indicates numerous inter-related difficulties with academic transcript transfers, such as inefficiency, secrecy, security, data integrity, and interoperability. These challenges are viewed from multiple angles, yet the literature does not provide a comprehensive answer that satisfies all criteria.

Data security is an important concern in academic transcript transfer. Data held in central databases or transmitted electronically is vulnerable to data loss, modification, fabrication, and unauthorised access to academic records (Alshahrani et al., 2022; Elisa et al., 2023). Blockchain technology still requires identity, access authorisation, and institutional permission, but it can provide a foundation for data integrity through distributed records and cryptographic verification.

Efficiency is another important challenge. Students from other universities are required to transfer and validate their academic records as quickly as possible (Cheung et al., 2021). Efficient transfer is vital for the running of institutions, but blockchain technology enables automatic verification with little or no human interference (Maestre et al., 2023). This can help reduce delays and the administrative burden associated with manual verification of academic records.

Interoperability is also a significant challenge. The free flow and interpretation of information could be limited by academic legislation, transcript formats and other publications, data structures, and information systems (Cheung et al., 2021; Smolenski, 2021). Therefore, interoperability is not only about connecting technology; it is also about shared data formats and regulations to ensure that academic information can be exchanged and interpreted consistently across institutions.

Data accuracy and transparency are further considerations in the transfer and verification of academic records. Chiş and Caramihai (2023) and Merlec et al. (2022) discuss the use of blockchain technology for verification and the tracking of reliable records. However, electronic degrees and portfolios are not the same as a full academic record with course-level grades, transferable credits, and comprehensible academic information. A complete academic transcript therefore requires mechanisms that support not only verification and traceability but also the accuracy and integrity of detailed academic information. Everything favours the interconnection of these themes. The immutable nature of blockchain and the audit trail it provides do not, on their own, solve the problems of data security, interoperability, and institutional authentication. Blockchain can provide a means of verifying and tracing records, but it still depends on appropriate institutional controls and accurate information being entered into the system. The findings therefore drive the requirements for the research design, including institutional authentication, controlled access, transcript fingerprinting, blockchain anchoring, verification, interoperability, duplicate prevention, and secure off-chain storage.

Blockchain Fundamentals

The first use of blockchain technology was launched with the Bitcoin whitepaper, and the technology has been adopted for applications beyond digital currency such as intelligent contracts, public services, the Internet of Things, reputation systems and security services (Kibet & Karume, 2018). A blockchain is just a chain of blocks. Each block is linked cryptographically to the previous one by pointing to the hash of the previous block. A cryptographic hash is a fixed-length value derived from the input data. This can be used as a digital fingerprint to identify any change in the data. Therefore, altering recorded information results in a new hash and may generate discrepancies in the next chain of references (Kibet & Karume, 2018; Leema et al., 2021).

Some blockchain elements are applicable to the transfer of academic transcripts. Decentralisation is a process of distributing the validation of transactions and the maintenance of the ledger to diverse members of the network instead of depending on a single central authority. This immutability makes it virtually impossible to change items on a blockchain backwards, once they are validated, without being caught. Pseudonymity uses blockchain addresses or IDs that do not immediately reveal a participant's real-world identity. Auditability refers to the ability to trace and audit recorded transactions via the transaction history kept by the network.

They have various implications for the transfer of transcripts. Cryptographic hashing can be used more generally to help with transcript integrity, as an institution can compare the fingerprint of the transcript it has received to the fingerprint it has already anchored on the blockchain. The decentralised validation can lessen the dependence on one central repository by dispersing the validation of transactions to several permitted organisations. Auditability gives a verifiable history of transactions associated with the transcript. But anonymity in itself does not give complete privacy, and immutability does not guarantee the accuracy of the information initially recorded on the blockchain.

This distinction is key in academic transcript management. A blockchain can store an incorrect or fraudulent record if an authorised participant provides incorrect information. Thus, the security of a transcript-transfer system depends on controls before information is attached to the ledger. Accordingly, this study integrates institutional authentication and authorisation with cryptographic fingerprinting and blockchain anchoring.

The literature also mentions the limits of blockchain technology. Scalability restrictions, the energy demands of proof-of-work consensus, public transparency of information on open ledgers, the susceptibility of small networks to majority attacks, and integration challenges with current systems have been identified by Kibet and Karume (2018). These constraints suggest that the use of blockchain is not inherently the right solution for every application. The network architecture, consensus method, access control, and data placement and integration needs should be evaluated simultaneously.

This privacy concern is especially relevant to academic transcripts. Student grades, credit information, identities and academic records are sensitive. Publishing full transcript contents on a public blockchain may disclose information to users other than intended. Literature consequently supports the separation between sensitive data and data for blockchain verification. In this work, the transcript contents are stored in protected off-chain storage, and a cryptographic fingerprint and restricted transaction information are

anchored to the blockchain. This way, blockchain technology can provide verification and integrity without storing full academic records on the ledger.

Blockchain Types and Consensus for Institutional Deployment

In general, there are three different types of blockchain networks: public, private and consortium. In a public blockchain, participation in viewing, sending, and validating transactions is usually open, according to the network's rules. A private blockchain limits participation and governance to a single organisation. A consortium blockchain (also known as a federated blockchain or a permissioned consortium network) allows a chosen set of companies to participate in governance and validate transactions (Kibet & Karume, 2018).

The distinctions between these setups are relevant for the maintenance of academic transcripts. Public networks are open and transparent, but they can expose transaction details in ways that are not appropriate for sensitive academic records. Private networks offer more institutional control, but centralise governance in a single entity. A consortium network shares validation across a number of authorised organisations, while managing the participants. This arrangement is thus compatible with a transcript-transfer setting including numerous higher education institutions and a suitable sector-level authority.

The research also suggests that the network type and the consensus process should be evaluated simultaneously. Proof of Work secures the network with computational expenses; however, it can have high energy consumption and transaction-processing costs (Kibet & Karume, 2018). Proof of stake reduces the computational load of proof of work, but presents governance issues due to stake distribution. In regulated situations where validators are recognisable and accountable, an alternative is Proof of Authority (Kibet, 2026b).

The necessary academic transcript transfer qualities are identifiable participants, regulated access, accountability and relatively predictable transaction volumes. Such features contrast with those of open Bitcoin networks, which require involvement by anonymous users. The literature therefore leans toward a permissioned setup, where approved institutions serve as validators and operate under pre-defined governance criteria. This study adopts this institutional approach by using a permissioned consortium design.

Smart Contracts and Modular Contract Design

Intelligent contracts make it possible to embed preset rules and execute them automatically on a blockchain. Smart agreements can automate contractual and procedural conditions and decrease the reliance on manual enforcement (Kibet et al., 2019). This feature is relevant to transcript transfer, as a number of operations, such as institutional registration, transcript registration, verification and access control, can be managed by established rules.

The literature also distinguishes between different types of smart-contract functions. Kibet et al. (2019) define storage database contracts, controller contracts for operations on stored information, contract-management contracts for coordinating components, application-logic contracts for domain-specific operations, and utility contracts for specialised reusable functions. This modular structure is different from a monolithic contract where all system functionalities are deployed within a single contract.

A modular method is crucial to academic transcript transfer since institutional regulations, verification procedures and data-exchange needs may evolve over time. Separation of storage, control and application logic can allow specific components to be changed without the need to rethink the whole system. The literature thus indicates that the smart-contract architecture should represent the functional organisation of the application and not just include all the blockchain operations in a single contract.

But intelligent contracts don't decide on their own if academic information is correct. They act upon the information and conditions given to them, and they implement rules. Therefore, if the source information is inaccurate, an incorrect transcript can be processed according to legitimate criteria. This constraint means that automating intelligent contracts must be supplemented with trusted institutional input and authentication.

The current project implements these findings in a modular architecture where institutional registration and transcript-related operations are governed using intelligent contracts. The design isolates the activities of institutional authorisation, transcript registration and verification. The blockchain layer facilitates the automated enforcement, while institutional actors are accountable for the accuracy of the academic material they submit.

Blockchain in Academic Credentialing

The literature has shown growing interest in applying blockchain to preserve, authenticate, and verify academic qualifications. But there are variances related to the kind of academic content, the network design and the specific issues of the various studies. The literature on blockchain-based solutions for academic certificate verification is expanding (Rustemi et al., 2023), but there is no empirical validation and practical deployment. Gaps are also to be found in live institutional installations, user-centred evaluation, interoperability testing and cost analysis. The limits reveal that the concept development went beyond the verification of operational success, and they point to the need for testing technical prototypes and functional evaluation in the present study.

Validation, Validity, and Equivalency of Institutional Accreditation and Academic Certification Architecture of Permissioned Blockchain for Authentication and Verification of Educational Credentials: Degree confirmation and traceability Chi and Caramihai, 2023. Rani et al. Alshahrani et al. (2022) Smart Certification in Higher Education with Blockchain; Al Hemaury et al. These studies highlight the use of Blockchain technology to increase authenticity, verification & traceability. Their major goal is to issue certificates, diplomas or certification processes and not to deliver full academic transcripts.

Merlec et al. (2022) proposed another solution: a consortium blockchain for managing electronic portfolios. Their effort is an example of how industry is collaborating to share information securely. However, this is not a standard academic transcript; it provides a wider range of information and does not need to match the formal credit recognition system by course level.

Alam (2022) considers information sharing on academic capability and advancement, while Smolenski (2021) considers certification from a broader policy and ecological perspective. The queries are not confined to individual credentials; they also cover mobility, exchange, and the valorisation of academic achievements. But official transcripts don't travel easily between schools. The recipient university validates the accuracy and completeness of the overall academic record and approves credits for prior learning.

Furthermore, Cheung et al. (2021) provide a way to regard cross-institutional credit transfer as an issue of information systems and academic processes. They conclude that organisations need to share academic material and engage in sense-making across institutions. Two topics come out together with the research on blockchain certification. The former is mostly about trust, authenticity and validation; the latter about flow of information, interoperability and acknowledgement of credit.

This distinction is important because an academic transcript is neither a certificate nor a diploma. A transcript is a comprehensive, cumulative record of a student's academic history, including courses undertaken, grades obtained, credits earned, and other evidence of academic achievement. In contrast, a certificate or diploma generally serves as formal confirmation that a particular qualification has been attained. Consequently, ensuring the authenticity of an academic transcript involves more than developing a mechanism to transmit a digital document. It requires institutional authorisation, regulated information exchange, verification of record integrity, interoperability between academic information systems, and recognition and transfer of academic credits. These requirements make academic transcript transfer a distinct problem from authenticating or verifying individual academic credentials.

The findings thus support an integrated transcript-transfer paradigm, not another stand-alone certificate-verification approach. This work connects the literature on cross-institutional credit transfer with the security and verification methodologies of the blockchain credentialing research. The technique is based on institutional authentication, role-based access control, cryptographic fingerprinting of transcripts, anchoring transcripts on the blockchain, validation using smart contracts, prohibition of duplicate records, transaction traceability, and secure off-chain storage. Table 1 summarises representative approaches against the dimensions of interest.

Table 1. Representative Approaches to Blockchain-Based Academic Credentialing

Study	Primary focus	Blockchain/network approach	Interoperability or integration focus	Record/credential level
Al Hemaury et al. (2024)	Validation, authentication and equivalency of academic certification and institutional accreditation	Blockchain-based framework and platform; specific implementation described in the study	Addresses academic certification validation and equivalency within the UAE context	Academic certification and institutional accreditation
Rani et al. (2024)	Educational certificate authentication and verification	Permissioned blockchain using Hyperledger Fabric	Focuses on certificate authentication and verification	Certificate level
Chiş and Caramihai (2023)	Traceability and verification of higher-education degrees	Blockchain-based secure traceability architecture	Addresses verification and traceability of degree credentials	Degree level
Maestre et al. (2023)	Application of blockchain algorithms to education certificate management	Blockchain-based certificate-management approach	Focuses on management and security of educational certificates	Certificate level
Alshahrani et al. (2022)	Blockchain-based smart certification for higher education	Blockchain-based smart certification system	Examines blockchain adoption for producing and sharing higher-education certificates	Certificate level
Merlec et al. (2022)	Secure and trusted electronic portfolio management	Consortium blockchain	Supports sharing of e-portfolio information across organisations	E-portfolio level
Cheung et al. (2021)	Cross-institutional credit transfer	Non-blockchain information-system approach	Directly addresses cross-institutional credit-transfer processes	Course and credit level
Present study	Secure academic transcript transfer and credit recognition	Permissioned consortium blockchain	Integrates institutional record management, blockchain verification and transcript exchange	Transcript, course and credit level

The works of Al Hemaury et al. (2024), Rani et al. (2024), Chiş and Caramihai (2023), Maestre et al. (2023) and Alshahrani et al. (2022) primarily address academic credentials, certificates and degrees, demonstrating the application of blockchain to authentication, verification, management and traceability. Merlec et al. (2022) extend this application to e-portfolios and demonstrate the potential of consortium blockchain for information exchange. Cheung et al. (2021) directly address cross-institutional credit transfer, but their approach is not blockchain-based. Consequently, existing studies provide useful insights into blockchain-enabled credential management and academic information exchange, but limited attention has been given to the specific challenges of secure, efficient and interoperable academic transcript transfer between institutions.

The investigations are not duplicative, but complementary. Studies on blockchain-based credentials provide techniques for building trust in academic knowledge, while cross-institutional transfer studies provide insight into the mobility and recognition of academic information. The distinction is that you need both dimensions to safely transfer transcripts. A system that only provides authenticity checking does not necessarily meet interoperability and credit-transfer requirements, and a system that only provides information interchange does not necessarily provide robust, tamper-evident verification.

This study addresses this gap by examining transfer from transcripts rather than confirmation of certificates or degrees. The model includes institutional record-keeping, controlled access, fingerprinting and verification via blockchain, smart-contract controls, and off-chain transcript storage. The contribution is then to add needs reported in the literature to one transcript-specific design.

Human and Organisational Factors

Technical controls do not work in a vacuum, separate from the people and organisations that utilise them. Kibet (2026a) identified human error, ignorance, and neglect as contributing factors to cybersecurity exposure in financial institutions. Although the study is outside the higher education sector, the findings may apply to this study, as academic transcript systems similarly rely on authorised staff to create, approve, send, and check information.

Regarding blockchain-based controls, the importance of human and organisational aspects is even more apparent. Although blockchain can make an authorised transaction traceable and resistant to retrospective manipulation, it cannot, on its own, determine whether the information provided by an authorised user is accurate. Similarly, the cryptographic protection cannot stop an authorised person from exchanging credentials, submitting the wrong record or falling for a social-engineering assault.

Therefore, the literature suggests that blockchain controls should be supplemented with institutional procedures and access-control measures. Role-based access can restrict system operations based on institutional responsibilities. Institutional authentication can identify which organisation can make a transaction. Transaction logs can be used as an accountability record of what was done in the system. These findings shape the present study by treating human and organisational variables as design considerations, not post-implementation concerns. The concept blends role-based access, institutional authorisation and transaction traceability with cryptography and blockchain restrictions.

Research Gap

The literature examined in this section shows that transferring academic transcripts faces interlinked difficulties related to security, efficiency, interoperability, integrity, and transparency. Studies on blockchain-based academic credentials show the promise of blockchain for authentication, verification and traceability, especially for certificates and degrees. However, the research on academic record exchange and credit transfer concerns the process of information transmission and acknowledgement of courses and credits between institutions.

However, the examined studies tackle these needs from diverse angles. Most studies on blockchain-based credentials focus on certificates, degrees, and other academic credentials. Cross-institutional credit transfer studies focus on exchanging and recognising academic records and credits. Thus, there is a gap in the integration of blockchain-based security and verification procedures with the transmission of detailed academic transcripts between higher education institutions.

The specific research gap addressed by this study is the lack of a combined transcript-specific model that combines institutional authorisation, cryptographic fingerprinting, blockchain-based verification, controlled transcript transfer, interoperability and protection of sensitive transcript information. Existing studies offer important mechanisms for credential verification or academic information exchange, but they do not integrate these requirements in a model specifically for academic transcript transfer.

This gap is addressed in the present work through the development of a blockchain paradigm for secure transfer of academic transcripts across higher education institutions. The model includes institutional authorisation, cryptographic fingerprinting, blockchain anchoring, smart-contract-based verification, duplicate prevention, transaction traceability, interoperability mechanisms and off-chain transcript storage. Credit transfer is viewed as a related process where information contained in the transferred transcript may help in the acknowledgement of already obtained academic credits, rather than a synonym of transcript transfer.

The contribution of the study is therefore to combine the security and verification mechanisms identified in blockchain-based credential research with the information-exchange requirements that have been identified in academic record and credit-transfer research, in a model that is specifically designed for the secure transfer and verification of academic transcripts.

3.0 METHODOLOGY

The study adopted a Design Science Research (DSR) strategy based on Peffers et al. (2007). The approach involved problem identification, specification of solution objectives, design and development, demonstration, assessment, and communication. DSR was used to identify challenges associated with academic transcript transfer, establish design requirements, develop the TransCrypt model, and provide a basis for evaluating its functionality through controlled technical testing. Design thinking was used as a supporting design activity within the design and development stage of DSR rather than as a separate methodology. The Empathise, Define, Ideate, Prototype, and Testing activities supported requirements identification, model development, and refinement. This approach maintained traceability between the identified problem, design requirements, developed artefact, and evaluation framework.

To achieve the first objective, a structured examination of literature on academic transcript and credit-transfer systems was conducted, with particular attention to security vulnerabilities, process inefficiencies, interoperability constraints, data integrity, and transparency. The review considered peer-reviewed journal articles, conference proceedings, systematic reviews, and policy publications addressing academic credentialing, credit transfer, and the use of blockchain in education. Preference was given to recent studies, systematic reviews, and research providing implementation or evaluation evidence, while foundational sources on blockchain architecture and consensus mechanisms were included where their technical principles remained relevant. Findings from the reviewed literature were classified into recurring problem categories and consolidated to establish the requirements that a secure academic transcript-transfer solution should address.

The second objective involved translating the identified challenges into the requirements and architecture of the proposed TransCrypt model. The requirements were considered from the perspectives of four stakeholder groups: students, academic registrars, system administrators, and receiving institutions. Blockchain capabilities were selected according to the identified requirements and structured into an architectural and operational model. Each design requirement was mapped to a corresponding architectural component to maintain traceability between the identified problem and the proposed solution. This ensured that each component of the model was supported by an identified requirement and that the requirements were addressed within the proposed architecture.

The study also developed a functional testing framework for subsequent prototype validation. Since the artefact developed in this study is an architectural model rather than a deployed system, the study does not present the proposed test cases as empirical evidence of system performance. Instead, the framework specifies test scenarios and expected results derived from the functional requirements of the model. It provides a basis for evaluating functions such as institutional authentication, authorisation, transcript fingerprinting, blockchain anchoring, verification, duplicate prevention, transaction traceability, and revocation when a prototype is implemented. The framework therefore provides a formal basis for subsequent functional validation of the proposed model (Kibet et al., 2022).

Ethical considerations were incorporated into the study because academic transcripts contain sensitive academic information. The study did not use personally identifying student information or involve human participants. It relied on literature, institutional policies, technical sources, and controlled demonstrations. The proposed model incorporates measures intended to protect academic information, including secure off-chain storage, cryptographic protection, access control, and controlled institutional participation. Confidentiality and data protection were therefore considered throughout the design and evaluation framework, alongside appropriate use and acknowledgement of scholarly sources.

4.0 FINDINGS AND DISCUSSION

Results for Objective One: Challenges in Academic Transcript Transfer

Five interrelated areas of concern for academic transcript transfer were highlighted: security, efficiency, interoperability, data integrity, and transparency. The results were not obtained through interviews with participants or an established institutional structure, but through synthesis of the research data.

Data security issues that may affect the legitimacy, secrecy, and integrity of academic records include unauthorised access, manipulation, falsification, and data loss (Alshahrani et al., 2022; Rani et al., 2010).

Manual verification, administrative procedures, and the transmission of academic content across institutions can cause efficiency problems, higher administrative workload, and longer processing times (Cheung et al., 2021; Maestre et al., 2023). Academic information uses several protocols and formats, and institutional information systems vary widely. These disparities create interoperability problems, i.e., the inability of organisations to exchange and interpret data (Cheung et al., 2021). Academic materials are vulnerable to change, raising concerns about the accuracy of the information conveyed and posing a risk to data integrity (Chiş & Caramihai, 2023; Rani et al., 2024). Transparency and third-party corroboration are equally vital. Research on the use of blockchain-based credentials has shown that verification and traceability are useful strategies to build confidence in scholarly information (Al Hemaury et al., 2024; Chiş & Caramihai, 2023).

Table 2. Challenges Identified in Academic Transcript Transfer

Challenge identified	Specific finding from the reviewed literature	Effect on transcript transfer
Security	Unauthorised access, tampering, forgery and data loss	Compromises confidentiality, integrity and authenticity of academic records
Efficiency	Manual verification and administrative procedures	May increase processing time and administrative workload
Interoperability	Differences in institutional systems, formats and academic conventions	Makes exchange and interpretation of transcripts more difficult
Data integrity	Academic information may be altered or manipulated	Reduces confidence in the accuracy and reliability of transferred records
Transparency	Verification may depend on the issuing institution or another trusted party	Makes independent verification and traceability more difficult

The results reveal that the difficulties are inter-related. Security and data-integrity mechanisms are needed to protect document validity, while efficiency and interoperability determine whether records can be transmitted and interpreted effectively. Transparency also helps build confidence by allowing the history of important transactions to be traced and verified. The results therefore show that no single solution fully satisfies the requirements for secure transmission of academic transcripts. The combined results were therefore used to establish the design requirements in the next section.

Results for Objective Two: Design Requirements

The second aim was to translate the issues found in the literature examined into design requirements for the model produced in this study. "The requirements were in the areas of secure access, transcript integrity, verification, participation on a controlled basis, interoperability, transparency, process automation, confidentiality and correction of superseded records.

Table 3. Design Requirements for the Blockchain-Based Academic Transcript Transfer Model

Design criterion	Challenge addressed	Blockchain-based response
DR1 Security of access control	Unauthorised access	Role-based authentication and authorisation
DR2 Transcript integrity	Unauthorised alteration	Cryptographic hash anchoring
DR3 Prevention of forgery	Forged academic records	Cryptographic fingerprinting and issuer verification
DR4 Automated verification	Verification delays	Smart-contract-based verification rules
DR5 Controlled decentralisation	Dependence on a single authority	Authorised institutional validation
DR6 Interoperability	Incompatible systems and formats	Standardised data exchange and common data structures
DR7 Transparency	Difficulty tracing transactions	Auditable transaction history
DR8 Data integrity	Alteration of academic records	Tamper-evident blockchain anchors
DR9 Process automation	Manual procedures	Smart-contract-mediated transfer workflow
DR10 Institutional usability	Difficulty adopting complex systems	Accessible interfaces for relevant institutional users
DR11 Data confidentiality	Exposure of student information	Protected off-chain transcript storage with on-chain fingerprints
DR12 Revocation and correction	Erroneous or superseded records	Status and supersession mechanism without rewriting the ledger

DR11 and DR12 are developed during the design phase based on the security and data-protection considerations identified in the literature. DR11 tackles the issue of protecting sensitive transcript information by separating the content of the transcript from the information required to verify the transcript on the blockchain. DR12 solves the practical problem of how to deal with incorrect or superseded entries, without changing past transactions on the blockchain. These standards complement the integrity of transcripts by saying that an academic record may need to be modified or replaced, while retaining an auditable record of changes.

Model Architecture

Layered Structure

The paradigm created in this study consists of five levels, including presentation, application, smart-contract, ledger and storage. The presentation layer offers interfaces for students, registrars, administrators and receiving institutions. The application layer is responsible for institutional integration, data mapping, notifications and other off-chain actions. The smart-contract layer enforces rules for authorisation, registering transcripts, transfer, and verification. The ledger layer stores the blockchain records and transaction history. The protected transcript documents are stored off-chain in the storage layer while their cryptographic fingerprints are stored on the blockchain.

This layered approach isolates the transcript's sensitive contents from the verification information stored on the blockchain and allows application-level processing outside the ledger while protecting the integrity of the on-chain anchoring information.

Smart Contract Design

The functional components are structured in the smart-contract layer for institutional registration, transcript anchoring, access control, transfer management and verification. The main contracts are InstitutionRegistry and TranscriptRegistry, which are supported by access-control and verification capabilities.

Table 4. Main Smart-Contract Functions of the Model

Contract/component	Main function
InstitutionRegistry	Registers authorised institutions and their identifiers
TranscriptRegistry	Records transcript fingerprints, issuer information, timestamps and status
Access Control	Restricts functions according to authorised roles
Transfer functions	Manage transcript-transfer requests, approvals and release
Verification functions	Compare a presented transcript fingerprint with the anchored fingerprint
Status/Revocation functions	Record superseded or revoked transcript status
Event functions	Record relevant transactions for traceability

The modular arrangement separates data management from operational logic and allows transcript registration, transfer and verification functions to be controlled independently. This improves maintainability and clarifies the relationship between functional requirements and blockchain components.

On-chain and Off-Chain Data Partitioning

A key architectural decision was separating transcript contents from blockchain verification data.

Table 5. On-Chain and Off-Chain Data Partitioning

Held on-chain	Held off-chain
Cryptographic transcript fingerprint	Transcript document
Issuing institution identifier	Student personal information
Timestamp	Supporting documents
Record status	Decryption keys
Relevant transaction information	Institutional academic records
Transfer and verification events	Rendered transcript files

The transcript is stored in safe, encrypted off-chain storage, and its cryptographic fingerprint and transaction details are anchored on the blockchain using SHA-256. SHA-256 creates a fixed 256-bit fingerprint. SHA-256 is a collision-resistant hash function: it is computationally infeasible for two separate inputs to produce the same hash. To verify, the fingerprint of the incoming transcript is recalculated and compared to the anchored fingerprint. If the two match, it means the document is the record previously anchored by the issuing institution. Any change results in a new fingerprint. This separation prevents direct

exposure of sensitive student information on the blockchain while maintaining integrity and traceability; repaired or replaced transcripts can be tagged as superseded with a new fingerprint while preserving the transaction history.

Network Configuration

The architecture is designed for a permissioned institutional blockchain environment where participating institutions are authorised before entering the network, and only authorised participants can issue transcripts, approve transfers, and verify. Validator nodes are run by accredited participating institutions and a designated sector regulator. Admission to a node requires institutional verification and approval from the network governance body. A validator can be suspended or removed when it breaks the network rules, its node becomes permanently unavailable, or its institutional authorisation is revoked. The regulator operates its own validator node, which supports governance, supervision, and network validation; other permitted validators handle temporary validator unavailability so transactions can proceed under the agreed consensus conditions. This permissioned approach allows restricted involvement, institutional accountability, and governance, while remaining consistent with the proposed academic transcript-transfer environment.

Identity and Access Control

The model uses role-based access control to limit the system functions according to institutional duties. The major positions are student, registrar, administrator and validator. Students apply for the transfer and obtain the required consent. Registrars perform authorised transcript-related actions. Administrators are responsible for the institutional setup. Verifiers check the validity of submitted transcripts against blockchain data. Application and smart contract-level access control provides another control against illegal actions. The transaction events are also documented for accountability and traceability.

Interoperability Layer

Interoperability is achieved by standardised data interchange between participating organisations. The architecture uses application programming interfaces and a standard data structure to transfer transcript data among institutional systems. The design also reflects the fact that technology compatibility alone does not erase differences in grading systems and credit methods. This preserves the original academic values and provides mapping information to aid interpretation by the receiving institution.

This matters because a transcript's legitimacy does not automatically determine how its credits or grades should be recognised. Thus, the receiving school remains responsible for making the correct academic recognition decision.

Operational Flow

The operating flow proceeds as follows:

1. A student logs into the system interface and requests to send a transcript to an institution, mentioning the institution to send it to and the record to transmit.
2. The request is evaluated and authorised by the academic registrar of the institution that issued the certificate.
3. The transcript is fetched, encrypted and stored off-chain.
4. IssuanceLogic binds its hash, issuer identity, pseudonymous student identifier and timestamp to the blockchain.

5. ConsentStore Records Student Consent, such as the receiving institution and Expiry
6. TransferLogic compares the request against the stored consent and registrar approval to release the decryption reference to the receiving institution.
7. The receiving institution receives the transcript, decrypts it, recomputes the hash of the transcript, and sends the hash to the VerificationLogic.
8. VerificationLogic compares the recomputed hash with the anchored value and returns a status of verified, superseded, revoked or not found.
9. The transaction records auditable events in the system, and the transfer history can be recreated by authorised stakeholders.

At every stage, error control is built in so faulty transactions do not go any farther. Rejected transactions occur due to failed authentication, lack of consent, unauthorised requests, faulty documents, duplicate records, unavailable storage or failed verification and an appropriate error status is noted for audit purposes. At step 8, verification does not require communication with the issuing institution, reducing dependency on third-party confirmation.

Proposed Evaluation Framework

The study, as completed, did not run functional tests on a deployed institutional system; hence the test cases provided here are a proposed evaluation framework, not evidence that the model is effective. The framework is designed on the basis of design requirements and defines functional tests that can be performed on a prototype implementation.

Table 6. Proposed Functional Evaluation Framework

ID	Functional test	Expected result
TC-01	Institutional user registration and role assignment	User is registered and the assigned role is enforced
TC-02	Transcript registration and fingerprint anchoring	Transcript fingerprint is recorded on-chain
TC-03	Verification of an unchanged transcript	Fingerprint matches the blockchain record
TC-04	Verification of an altered transcript	Fingerprint does not match and verification fails
TC-05	Student transfer request and registrar approval	Request requires authorised approval before release
TC-06	Access without valid authorisation	Access is denied
TC-07	Expired transfer authorisation	Access is no longer permitted
TC-08	Supersession of an incorrect transcript	Previous record is marked superseded and new record is maintained
TC-09	Cross-institution transcript retrieval	Authorised receiving institution can retrieve the record
TC-10	Interoperability of transcript data	Data can be exchanged using the defined structure
TC-11	Unauthorised institutional transaction	Transaction is rejected
TC-12	Transaction-history verification	Relevant transfer activities can be traced

The framework provides a methodical basis for future prototype validation by associating each test case with a corresponding functional need. But the test cases themselves do not demonstrate that the model has passed the tests. Real effectiveness can only be determined by implementing and running the specific tests using relevant test data and a working prototype.

Discussion

Traceability from Challenge to Component

The results of goal one indicates that transcript transfer is not only a record delivery difficulty but also a security, process and systems integration problem. Security deficiencies affect the integrity and confidentiality of records, manual processes create delays and administrative overhead, and interoperability limitations restrict the ability to share and understand records consistently. The results show that it is necessary to find a solution to the difficulties as a whole, and not as discrete problems.

Each is answered by the model defined in objective two. The ledger provides the distributed, tamper-evident record layer; cryptographic hashing provides integrity and independent verification; intelligent contracts automate the request, approval and release process; distributed validation across a consortium removes dependence on a single attesting party; and the three-level interoperability layer addresses transport, syntax and semantics. The traceability is shown explicitly in Table 7.

Table 7. Traceability from Identified Challenge to Architectural Component

Challenge	Design requirements	Architectural components
Security	DR1, DR3, DR11	AccessControl, role model, off-chain encryption, issuer signature verification
Efficiency	DR4, DR9	IssuanceLogic, TransferLogic, off-chain workers, batched anchoring
Interoperability	DR6	REST APIs, common credential schema, credit and grading mapping service
Data integrity	DR2, DR8, DR12	TranscriptAnchorStore, VerificationLogic, supersession status registry
Transparency	DR5, DR7	Consortium validation, EventLogger, auditable event history

Consensus and Network Design

The choice of consensus mechanism is also a governance decision because the validator set determines who can participate in transaction validation, shares responsibility for maintaining the ledger, and responds to network-related problems. This distributes responsibility among accountable parties and supports coordinated transcript verification (Kibet, 2026b). Governance may therefore involve a sector regulator and a consortium of recognised institutions. However, institutions may hesitate to participate because of concerns about implementation costs, technological capacity, data sharing, and potential loss of control over academic records. The proposed permissioned approach addresses these concerns by limiting network participation, clarifying institutional responsibilities, distributing governance responsibilities, storing sensitive documents off-chain, and providing standardised interfaces that allow

institutions to retain control of their underlying academic information systems. This approach enables distributed validation while preserving institutional responsibility and regulatory oversight.

Privacy and Data Protection

Separating personal data from the blockchain ledger reduces direct exposure of sensitive student information, but two additional privacy considerations remain. First, using a pseudonymised on-chain identifier across multiple records may enable correlation of transactions associated with the same student. When combined with auxiliary information, such correlation may create a risk of re-identification (Kibet & Karume, 2018). Where the consortium structure increases this risk, measures such as periodic rotation of identifiers or the use of institution-specific identifiers should be considered.

Second, although auditability strengthens accountability, it may also create a persistent record of the institutions to which a student has requested transcript transfers and when those requests were made. Such information may be sensitive, particularly where a transfer request is unsuccessful. Transfer-related events should therefore be accessible only to authorised parties directly involved in the transaction rather than being visible across the entire consortium. The architecture should therefore incorporate appropriate event-level access controls to balance auditability with student privacy.

Human and Organisational Factors

The findings suggest that non-compliant behaviour may contribute significantly to organisational cybersecurity exposure, with negligence identified as a prominent factor (Kibet, 2026b). The proposed architecture remains subject to similar human and organisational risks, particularly in relation to the management of registrar credentials, the accuracy of records generated by institutional academic management systems, and adherence to appropriate administrative procedures. Cryptographic controls cannot prevent an authorised user from anchoring an incorrect record; they only ensure that the anchored record remains unchanged after registration. Accordingly, the design incorporates segregation of responsibilities between issuing and approving personnel, secure key storage, mandatory review before anchoring, and periodic reconciliation with the source system. Registrars and administrators should also receive appropriate training and competency assessment in secure transcript handling, access control, key management and verification procedures. These measures strengthen accountability and embed safe practices within the operational process rather than relying solely on individual awareness.

Comparison with Existing Approaches

The proposed technique differs from the certificate-oriented systems in Table 1 in three ways. It works at course and credit level rather than qualification level – the level at which credit transfer decisions are actually made. It does not assume that verifying authenticity is sufficient for recognition; instead, it treats semantic interoperability as a first-class requirement with a specific mapping service. And it recognises supersession as an important process, noting that transcripts (unlike terminal certificates) are amended throughout and after a program of study.

The concept maintains the integration focus of non-blockchain credit transfer information systems (Cheung et al., 2021). Still, it removes the necessity for the receiving institution to trust the sending institution's system, or a central intermediary, to confirm what it receives.

Limitations

Four constraints must be acknowledged. First, the artefact is an architectural model rather than a deployed system. Although a functional evaluation framework has been proposed, it has not yet been implemented. Therefore, claims regarding the model's performance, usability and institutional acceptance remain subject to future empirical evaluation. In line with Design Science Research principles, the contribution of an artefact should be demonstrated through systematic evaluation, which remains a task for subsequent research.

Secondly, the problem synthesis is based on a structured assessment, rather than primary data collection from registry offices. Practitioner interviews or process observation would probably reveal operational limits like system limitations, archive record quality, personnel and workload patterns that the research does not capture.

Third, the architecture implies that a consortium may be convened; The design does not specify how such a consortium would be administered, funded or expanded. Establishing a validator set among certified institutions and a regulator is an institutional and political task at least as demanding as the technical one.

Fourth, the interoperability treatment assumes that credit and grading procedures are convertible to a common reference frame. Institutions vary in size and in what a credit means in terms of contact hours and measured learning outcomes; thus mapping is an approximation and academic judgement at the receiving institution is still needed.

5.0 CONCLUSION AND RECOMMENDATIONS

Conclusion: The study revealed that security, efficiency, interoperability, data integrity and transparency were the top concerns affecting the transfer of academic transcripts. Traditional techniques, including paper, email and centralised systems, leave records vulnerable to unwanted access, manipulation and delay, and increase administrative burden. This led the study to propose a blockchain-based paradigm that integrates distributed validation, cryptographic hashing, smart contracts, blockchain anchoring, standardised data exchange, and transparent transaction records. The model uses a permissioned consortium network governed by recognised institutions and a sector regulator. Sensitive information in the transcript is stored in off-chain protected storage. The study indicates that blockchain can offer tamper-evident transcript verification and traceability without the requirement of storing the entire academic data on the blockchain.

Recommendations: Institutions of higher education should examine the use of defined data formats and compatible interfaces to assist secure transmission of transcripts between different academic information systems. Institutions participating in a permissioned blockchain network should establish governance procedures for validator admission, access control, responsibilities, accountability, and data protection. Registrars and administrators should get sufficient training in secure transcript processing, authentication, key management and verification procedures. Future implementations have to consider the cost, scalability, regulatory compliance and organisational readiness to develop a consortium-based transcript-transfer system.

Further research should focus on developing and evaluating a functional prototype using the test cases outlined in this study. Future studies could include primary data collection from register offices to validate

and broaden the operational problems found. Future studies should examine consortium governance, finance, validator engagement, and institutional uptake. Further work on semantic interoperability is also needed, particularly mapping credits, grading systems, and academic requirements between schools.

6.0 REFERENCES

1. Al Hemaury, M., Abu Talib, M., Khalil, A., Zulfikar, A., & Mohamed, T. (2024). Blockchain-based framework and platform for validation, authentication & equivalency of academic certification and institution's accreditation: UAE case study and system performance. *Education and Information Technologies*, 29, 18203–18232. <https://doi.org/10.1007/s10639-024-12493-6>
2. Alam, A. (2022). Platform utilising blockchain technology for eLearning and online education for open sharing of academic proficiency and progress records. In R. Asokan, D. P. Ruiz, Z. A. Baig, & S. Piramuthu (Eds.), *Smart data intelligence: Proceedings of ICSMDI 2022* (pp. 307–320). Springer Nature Singapore. https://doi.org/10.1007/978-981-19-3311-0_26
3. Alshahrani, M., Beloff, N., & White, M. (2022). Towards a blockchain-based smart certification system for higher education: An empirical study. *International Journal of Computing and Digital Systems*, 11(1), 553–571. <https://doi.org/10.12785/ijcds/110145>
4. Cheung, K., Li, B., Benz, P., Chow, K.-M., Ng, J. T. D., Kwok, W. Y. Y., Tsang, H., Leung, D. N. H., Lui, J. K. Y., Li, Y. N., So, P. Y., & Leung, A. (2021). Prototype development of a cross-institutional credit transfer information system for community college transfer students. *Sustainability*, 13(16), Article 9398. <https://doi.org/10.3390/su13169398>
5. Chiş, D., & Caramihai, M. (2023). Blockchain in higher education: A secure traceability architecture for degree verification. In S. Mistretta (Ed.), *Reimagining education: The role of e-learning, creativity, and technology in the post-pandemic era*. IntechOpen. <https://doi.org/10.5772/intechopen.1001997>
6. Elisa, N., Yang, L., Chao, F., & Cao, Y. (2023). A framework of blockchain-based secure and privacy-preserving e-government system. *Wireless Networks*, 29(3), 1005–1015. <https://doi.org/10.1007/s11276-018-1883-0>
7. Kibet, A. (2026a). Assessing human-induced cybersecurity risk using a human vulnerabilities exposure index (CSHVEI). *Open Journal of Applied Sciences*, 16(2), 696–717. <https://doi.org/10.4236/ojapps.2026.162043>
8. Kibet, A. (2026b). A design science study of blockchain-based governance and incentive architectures for ride-sharing platforms. *Open Journal of Applied Sciences*, 16(1), 300–319. <https://doi.org/10.4236/ojapps.2026.161019>
9. Kibet, A., & Karume, S. M. (2018). A synopsis of blockchain technology. *International Journal of Advanced Research in Computer Engineering & Technology*, 7(11), 789–795. https://www.researchgate.net/publication/329358619_A_Synopsis_of_Blockchain_Technology
10. Kibet, A., Karume, S., & Masese, N. (2022). Functional testing on a software model for creating a stable cryptocurrency using fiat currency for global electronic commerce. *International Journal for Research in Applied Science & Engineering Technology*, 10(10), 236–240. <https://doi.org/10.22214/ijraset.2022.46682>
11. Kibet, A., Thiga, M. M., & Karume, S. M. (2019). Towards a blockchain based smart contracts model design for housing market applications. *International Journal of Advanced Research in Computer Engineering & Technology*, 8(8), 318–326. <http://ijarcet.org/wp-content/uploads/IJARCET-VOL-8-ISSUE-8-318-326.pdf>

12. Leema, R. G., Rajmohan, R., Usharani, S., Kiruba, K., & Manjubala, P. (2021). Fundamentals of blockchain and distributed ledger technology (DLT). In A. K. Tyagi & A. Abraham (Eds.), *Recent trends in blockchain for information systems security and privacy* (pp. 3–38). CRC Press. <https://doi.org/10.1201/9781003139737-2>
13. Maestre, R. J., Bermejo Higuera, J., Gámez Gómez, N., Bermejo Higuera, J. R., Sicilia Montalvo, J. A., & Orcos Palma, L. (2023). The application of blockchain algorithms to the management of education certificates. *Evolutionary Intelligence*, 16(6), 1967–1984. <https://doi.org/10.1007/s12065-022-00812-0>
14. Merlec, M. M., Islam, M. M., Lee, Y. K., & In, H. P. (2022). A consortium blockchain-based secure and trusted electronic portfolio management scheme. *Sensors*, 22(3), Article 1271. <https://doi.org/10.3390/s22031271>
15. Rani, P., Sachan, R. K., & Kukreja, S. (2024). Educert-chain: A secure and notarized educational certificate authentication and verification system using permissioned blockchain. *Cluster Computing*, 27(7), 10169–10196. <https://doi.org/10.1007/s10586-024-04469-5>
16. Rustemi, A., Dalipi, F., Atanasovski, V., & Risteski, A. (2023). A systematic literature review on blockchain-based systems for academic certificate verification. *IEEE Access*, 11, 64679–64696. <https://doi.org/10.1109/ACCESS.2023.3289598>
17. Smolenski, N. (2021). Blockchain for education: A new credentialing ecosystem. In *OECD Digital education outlook 2021: Pushing the frontiers with artificial intelligence, blockchain and robots* (pp. 209–234). OECD Publishing. <https://doi.org/10.1787/589b283f-en>